

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application.

1. **(Currently amended)** A communication authorization method, comprising:
a third party server receiving a request for access information to access content;
generating the access information and session rights to access the desired content from a first application server;
generating authentication of the access information and session rights using a first service ticket to the first application server, wherein the first service ticket is obtained from a key distribution center (KDC), wherein the KDC is a separate entity from the first application server; and
sending the access information, session rights and authentication to a client, whereby the client presents the access information, session rights and authentication to the first application server to be authorized to receive the desired content from the first application server;
the method further comprising:
the first application server receiving a key request including the access information and authentication;
extracting the access information and authentication;
verifying the authentication of the access information using the first service ticket, and client authorization; and
issuing a key reply if the authentication of the access information and client authorization are verified.

2. **(Canceled)**

3. **(Previously presented)** The method as claimed in claim 1, further comprising:

encrypting at least a portion of the session rights using a third party server session key for the first application server.

4. (Canceled)

5. (Previously presented) The method as claimed in claim 1, further comprising:

- requesting a ticket granting ticket (TGT ticket);
- receiving a TGT ticket;
- requesting the first party server service ticket for the first application server; and
- receiving the first party server service ticket for the first application server.

6. (Currently amended) The method as claimed in claim 1, further comprising:
~~the first application server receiving a key request including the access information and authentication;~~

- ~~extracting the access information and authentication;~~
- ~~verifying the authentication of the access information using the first service ticket, and client authorization;~~
- ~~issuing a key reply if the authentication of the access information and client authorization are verified;~~

- the KDC receiving a second service ticket request from a client for the first application server;

- issuing a second service ticket for the first application server; and

- the step of the first application server receiving a key request from a client wherein the key request includes the second service ticket.

7. (Previously presented) The method as claimed in claim 6, further comprising:

- a client generating a key request including the access information and the authentication;

- sending the key request to the first application server; and

receiving the key reply (KEY_REP) if the authentication of the access information and client authorization are verified by the first application server.

8. **(Currently amended)** A method for verifying authorization for a client to gain access to content and/or services, comprising:

- receiving a key request from a client;
- extracting third party server access information, session rights and third party server authentication from the key request;
- verifying an authentication of the third party access information, session rights and a client authorization;
- issuing a key reply directly to the client if the authentication of the third party access information, session rights and the client authorization are verified;
- ~~the KDC receiving, in a key distribution center (KDC), wherein the KDC is a separate entity from an application server,~~ a second service ticket request from a client for the application server;
- issuing a second service ticket for the application server; and
- the step of the application server receiving a key request from a client wherein the key request includes the second service ticket.

9. **(Previously presented)** The method as claimed in claim 8, further comprising:

- authenticating the third party server access information using the third party server authentication.

10. **(Previously presented)** The method as claimed in claim 9, wherein the authenticating includes extracting a first service ticket and authenticating the third party server access information using the first service ticket.

11. **(Previously presented)** The method as claimed in claim 8, wherein the extracting the third party server authentication, further comprising the steps of extracting a session key from the first party ticket included in the key request; and the step of

authenticating the access information includes verifying a third party server signature using the session key.

12. **(Previously presented)** The method as claimed in claim 11, wherein the extracting the session key includes decrypting at least a portion of the first party ticket included in the key request using the first application server service key and extracting the session key.

13. **(Previously presented)** The method as claimed in claim 5, further comprising:

- the third party server receiving a request for the access information to access content;
- generating the third party server access information to access the desired content from a first application server; and
- generating the third party server authentication of the access information.

14. **(Previously presented)** The method as claimed in claim 13, wherein the generating the third party server authentication includes incorporating a first party server service ticket for the first application server.

15. **(Previously presented)** The method as claimed in claim 14, wherein the generating the authentication includes generating a signature utilizing a session key of the first party server service ticket.

16. **(Canceled)**

17. **(Currently amended)** A method for providing secure communication when distributing services, comprising:

- a third party server receiving a selection for services;
- issuing access information and session rights for the services;
- issuing authentication of the access information and the session rights;

an application server receiving a key request from a client, the key request including the access information and authentication;

extracting the access information and authentication;

verifying an authentication of the access information, session rights and a client authorization utilizing, at least in part, a first service ticket; and

issuing a key reply directly to a client if the authentication of the access information, session rights and the client authorization are verified.

18. **(Previously presented)** The method as claimed in claim 17, further comprising:

a KDC receiving a first service ticket request from a third party server for the first application server;

the KDC issuing the first service ticket to the third party server for the first application server; and

the steps of the third party server issuing access information and authentication including generating the access information and authentication using the first service ticket.

19. **(Previously presented)** The method as claimed in claim 17, further comprising:

the KDC receiving a second service ticket request from a client for the first application server;

issuing a second service ticket for the first application server; and

the step of the application server receiving a key request from a client wherein the key request includes the second service ticket.

20. **(Previously presented)** The method as claimed in claim 17, wherein: the verifying the authentication of the access information includes:

extracting the first service ticket;

decrypting the first service ticket;

extracting a session key from the first service ticket;

generating a signature using the session key; and
verifying the signature over the access information with the session key.